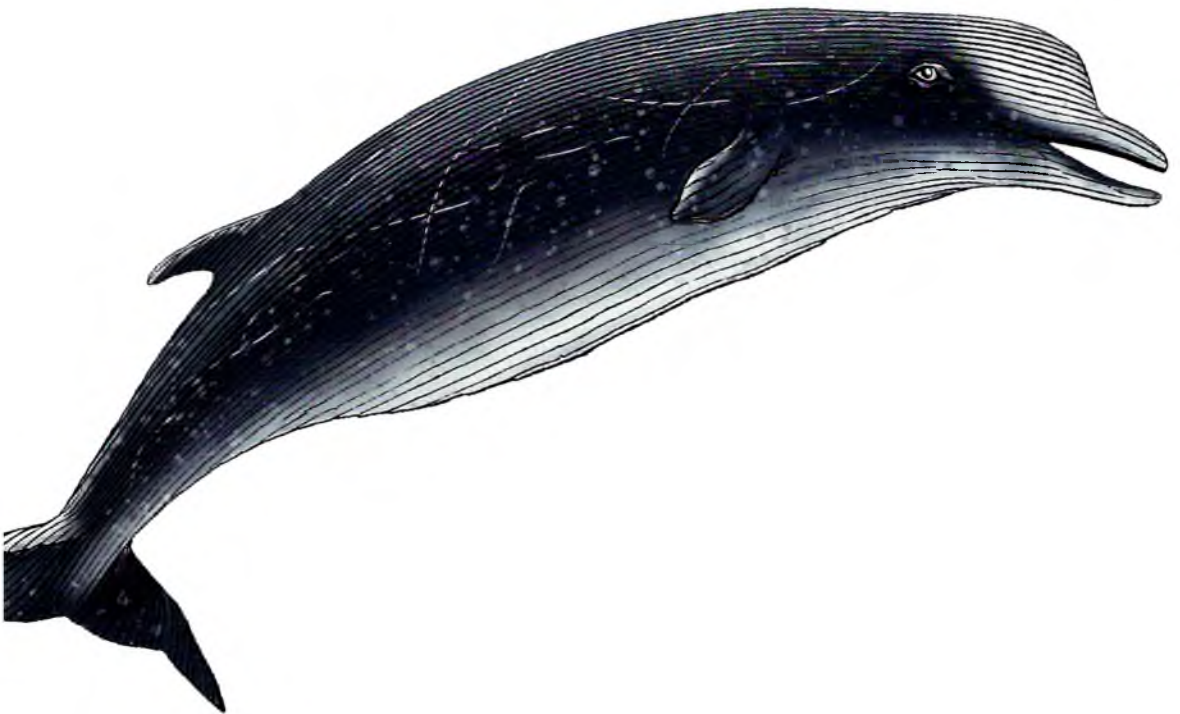


O'REILLY®

# Kubernetes на практике

Создание успешных платформ приложений



Джош Россо, Рич Ландер,  
Александр Бранд, Джон Харрис

---

# Оглавление

<b>Предисловие</b> .....	<b>13</b>
<b>Введение</b> .....	<b>15</b>
Условные обозначения .....	16
Использование примеров кода .....	17
Платформа онлайн-обучения O'Reilly .....	18
Благодарности .....	18
<b>ГЛАВА 1. Путь к эксплуатации</b> .....	<b>21</b>
Что такое Kubernetes .....	21
Основные компоненты .....	22
Не только оркестрация: дополнительные функции .....	24
Интерфейсы Kubernetes .....	24
Kubernetes в целом .....	26
Что такое платформа приложений .....	27
Спектр подходов .....	28
Спектр подходов с учетом потребностей вашей организации .....	29
Платформы приложений: подводим итоги .....	31
Создание платформ приложений на основе Kubernetes .....	31
Начиная снизу .....	33
Спектр абстрагирования .....	34
Определение возможностей платформы .....	36
Составные компоненты .....	37
Резюме .....	41
<b>ГЛАВА 2. Модели развертывания</b> .....	<b>42</b>
Управляемые сервисы и самостоятельное развертывание .....	42
Управляемые сервисы .....	43
Самостоятельное развертывание .....	43
Принятие решения .....	44
Автоматизация .....	45
Готовый установщик .....	45
Собственные средства автоматизации .....	46

Архитектура и топология .....	47
Модели развертывания etcd .....	47
Уровни кластера .....	49
Пулы узлов .....	50
Федерация кластеров .....	52
Инфраструктура .....	55
Физическое и виртуальное оборудование .....	56
Выбор размера для кластера .....	59
Вычислительная инфраструктура .....	61
Сетевая инфраструктура .....	62
Стратегии автоматизации .....	64
Развертывание серверов .....	66
Управление конфигурацией .....	66
Системные образы .....	67
Что устанавливать .....	67
Контейнерные компоненты .....	69
Дополнения .....	70
Обновления .....	72
Версионирование платформы .....	73
Планирование на случай сбоев .....	73
Интеграционное тестирование .....	74
Стратегии .....	75
Механизмы инициирования .....	81
Резюме .....	82
<b>ГЛАВА 3. Среда выполнения контейнеров .....</b>	<b>83</b>
Появление контейнеров .....	83
Open Container Initiative .....	85
Спецификация OCI для сред выполнения .....	85
Спецификация OCI для образов .....	87
Интерфейс среды выполнения контейнеров .....	90
Запуск Pod'a .....	90
Выбор среды выполнения .....	92
Docker .....	93
containerd .....	94
CRI-O .....	95
Kata Containers .....	96
Virtual Kubelet .....	98
Резюме .....	98
<b>ГЛАВА 4. Хранилище данных контейнера .....</b>	<b>100</b>
Требования к хранилищу .....	100
Режимы доступа .....	101
Расширение томов .....	101
Выделение томов .....	102

Резервное копирование и восстановление.....	102
Блочные устройства и хранение файлов/объектов .....	103
Временные данные .....	103
Выбор провайдера хранилища.....	104
Механизмы для работы с хранилищами в Kubernetes .....	104
Постоянные тома и заявки на выделение .....	104
Классы хранилищ.....	107
CSI .....	108
Контроллер CSI.....	109
Узел CSI.....	110
Реализация хранилища в виде сервиса.....	110
Установка компонентов CSI .....	110
Предоставление разных вариантов хранилищ .....	113
Использование хранилища.....	115
Изменение размера .....	117
Копии (snapshots).....	118
Резюме.....	120
<b>ГЛАВА 5. Сетевое взаимодействие между Pod'ами .....</b>	<b>121</b>
Аспекты, связанные с сетью .....	122
Управление IP-адресами .....	122
Протоколы маршрутизации .....	124
Инкапсуляция и туннелирование .....	126
Маршрутизируемость приложений.....	127
IPv4 и IPv6 .....	128
Шифрование трафика рабочих заданий.....	128
Сетевая политика .....	129
Аспекты, связанные с сетью: итоги .....	131
Интерфейс управления сетью контейнеров (CNI).....	132
Установка CNI.....	133
Подключаемые модули CNI.....	136
Calico .....	136
Cilium .....	140
AWS VPC CNI.....	143
Multus .....	144
Дополнительные подключаемые модули .....	145
Резюме.....	146
<b>ГЛАВА 6. Маршрутизация сервисов .....</b>	<b>147</b>
Сервисы Kubernetes.....	148
Компонент Service .....	148
Endpoints .....	154
Аспекты реализации Сервиса .....	158
Обнаружение сервисов .....	168
Производительность DNS-сервиса.....	170

Ingress .....	172
Зачем нужен механизм Ingress.....	172
API-интерфейс Ingress .....	173
Контроллеры Ingress и принцип их работы .....	176
Методы маршрутизации входящего трафика.....	177
Выбор контроллера Ingress .....	181
Вопросы, связанные с развертыванием контроллера Ingress .....	183
DNS-сервер и его роль в обработке входящего трафика .....	185
Управление сертификатами TLS .....	187
Mesh-сеть .....	189
Где (не) следует использовать mesh-сети.....	190
Интерфейс mesh-сети .....	191
Прокси-сервер плоскости данных .....	194
Mesh-сеть в Kubernetes .....	196
Архитектура плоскости данных .....	201
Внедрение mesh-сети.....	202
Резюме.....	206
<b>ГЛАВА 7. Управление конфиденциальными данными .....</b>	<b>207</b>
Углубленная защита .....	208
Шифрование дисков .....	209
Безопасность во время передачи .....	210
Прикладное шифрование .....	211
Secret API в Kubernetes .....	211
Модели потребления объектов <i>Secret</i> .....	213
Конфиденциальные данные в etcd.....	216
Шифрование с использованием статического ключа.....	218
Шифрование методом конвертов .....	222
Внешние провайдеры.....	224
Vault.....	224
Cyberark.....	225
Интеграция путем внедрения.....	225
Интеграция CSI .....	230
Конфиденциальные данные в декларативном мире .....	232
Запечатывание конфиденциальных данных.....	233
Обновление ключей.....	236
Многокластерные модели .....	237
Рекомендации по работе с конфиденциальными данными .....	237
Всегда проводите аудит взаимодействия с конфиденциальными данными .....	238
Не раскрывайте конфиденциальные данные.....	238
Отдавайте предпочтение томам перед переменными окружения.....	238
Делайте так, чтобы ваши приложения не знали о провайдерах хранилищ для конфиденциальных данных .....	239
Резюме.....	239

<b>ГЛАВА 8. Управление допуском.....</b>	<b>240</b>
Цепочка допуска в Kubernetes .....	241
Встроенные контроллеры допуска .....	242
Веб-хуки.....	243
Настройка контроллеров допуска на основе веб-хуков .....	245
Аспекты проектирования веб-хуков .....	247
Написание изменяющего веб-хука .....	248
Простой HTTPS-обработчик.....	249
Controller Runtime .....	251
Системы с централизованными политиками.....	254
Резюме.....	261
<b>ГЛАВА 9. Наблюдаемость .....</b>	<b>262</b>
Принцип работы журналирования .....	262
Обработка журнальных записей контейнера .....	263
Журналы аудита в Kubernetes.....	266
События Kubernetes .....	268
Генерация оповещений на основе журнальных записей.....	270
Последствия для безопасности .....	270
Метрики .....	270
Prometheus.....	271
Долгосрочное хранение.....	272
Пассивная модель сбора метрик.....	272
Пользовательские метрики .....	273
Организация метрик и федеративные системы.....	274
Оповещения .....	275
Потребляемые ресурсы и их стоимость.....	276
Компоненты для работы с метриками .....	280
Распределенная трассировка.....	288
OpenTracing и OpenTelemetry .....	289
Компоненты трассировки.....	290
Инструментирование приложений.....	291
Mesh-сети.....	291
Резюме.....	292
<b>ГЛАВА 10. Идентификация .....</b>	<b>293</b>
Идентификация пользователей.....	294
Методы аутентификации.....	295
Выдача пользователям минимальных привилегий.....	306
Идентификация контейнерных приложений.....	309
Общие секреты.....	310
Сетевая идентификация.....	311
Токены служебной учетной записи.....	315

Прогнозируемые токены служебной учетной записи .....	318
Идентификация узлов на уровне платформы.....	321
Резюме.....	333
<b>ГЛАВА 11. Создание сервисов платформы .....</b>	<b>335</b>
Механизмы расширения .....	336
Подключаемые расширения.....	336
Расширения на основе веб-хуков .....	337
Операторы .....	338
Шаблон проектирования "оператор".....	339
Контролеры Kubernetes .....	339
Пользовательские ресурсы.....	341
Сценарии использования операторов .....	344
Служебные компоненты платформы .....	345
Операторы приложений общего назначения.....	346
Операторы для отдельно взятых приложений .....	346
Разработка операторов.....	347
Инструментарий для разработки операторов.....	347
Проектирование моделей данных .....	351
Реализация бизнес-логики.....	353
Расширение планировщика .....	370
Предикаты и приоритеты .....	370
Политики планирования.....	371
Профили планирования .....	372
Несколько планировщиков .....	373
Создание собственного планировщика.....	373
Резюме.....	373
<b>ГЛАВА 12. Мультитенантность .....</b>	<b>374</b>
Уровни изоляции.....	374
Однотенантные кластеры.....	375
Мультитенантные кластеры.....	376
Разделение на основе пространств имен.....	377
Мультитенантность в Kubernetes.....	379
Управление доступом на основе ролей.....	379
Квоты на ресурсы.....	381
Веб-хуки допуска.....	382
Запросы и лимиты на ресурсы.....	384
Сетевые политики .....	389
Политики безопасности Pod .....	392
Сервисы мультитенантных платформ.....	395
Резюме.....	397

<b>ГЛАВА 13. Автоматическое масштабирование .....</b>	<b>398</b>
Виды масштабирования.....	399
Архитектура приложения.....	400
Автомасштабирование приложений .....	401
Horizontal Pod Autoscaler .....	401
Vertical Pod Autoscaler .....	405
Автомасштабирование с помощью пользовательских метрик.....	408
cluster-proportional-autoscaler .....	409
Создание собственных средств автомасштабирования.....	410
Автомасштабирование кластера.....	410
Выделение резервных ресурсов для кластера .....	414
Резюме.....	416
<b>ГЛАВА 14. Эффективная эксплуатация приложений .....</b>	<b>417</b>
Развертывание приложений в Kubernetes .....	418
Шаблонизация манифестов развертывания .....	418
Упаковка приложений для Kubernetes .....	419
Получение конфигурации и конфиденциальных данных .....	419
Объекты <i>ConfigMap</i> и <i>Secret</i> .....	420
Получение конфигурации из внешних систем.....	423
Реакция на события перепланирования .....	424
Хуки, срабатывающие перед остановкой контейнеров.....	424
Безопасное завершение работы контейнеров.....	425
Удовлетворение требований доступности.....	427
Проверки состояния .....	429
Проверки работоспособности .....	429
Проверки готовности.....	430
Проверки состояния запуска.....	431
Реализация проверок .....	432
Запросы и лимиты на ресурсы Pod.....	432
Запросы ресурсов .....	433
Лимиты на ресурсы.....	434
Журналирование приложений .....	434
Что записывать в журнал .....	435
Структурированные и неструктурированные журнальные записи.....	435
Контекстная информация в журнальных записях .....	436
Предоставление метрик.....	436
Инструментирование приложений.....	436
Метод USE.....	438
Метод RED .....	438
Четыре "золотых" сигнала .....	439
Метрики отдельных приложений.....	439

Инструментирование сервисов для распределенной трассировки.....	439
Инициализация трассировщика.....	440
Создание спанов.....	441
Передача контекста.....	442
Резюме.....	443
<b>ГЛАВА 15. Логистика доставки программного обеспечения .....</b>	<b>444</b>
Создание образов контейнеров.....	445
Плохая практика "золотых" базовых образов .....	447
Выбор базового образа .....	448
Выбор пользователя для выполнения контейнера.....	449
Явное определение версий пакетов.....	450
Образы для сборки и выполнения приложений.....	450
Cloud Native Buildpacks .....	451
Реестры образов .....	453
Сканирование уязвимостей.....	454
Процедура карантина .....	456
Подписание образов .....	457
Непрерывная доставка.....	458
Интеграция процесса сборки в конвейер.....	459
Развертывание на основе загрузки .....	462
Методы выкатывания изменений .....	464
GitOps.....	466
Резюме.....	467
<b>ГЛАВА 16. Абстрагирование платформы.....</b>	<b>469</b>
Открытость платформы.....	469
Самостоятельное присоединение к платформе.....	471
Спектр абстрагирования.....	473
Инструменты командной строки.....	474
Абстрагирование посредством шаблонизации .....	475
Абстрагирование стандартных компонентов Kubernetes.....	479
Полностью скрываем Kubernetes.....	482
Резюме.....	485
<b>Об авторах .....</b>	<b>487</b>
<b>Об изображении на обложке .....</b>	<b>488</b>
<b>Предметный указатель .....</b>	<b>489</b>